REMARKS

Claims 1-10, 13, 15-17, 19, 21 and 22 are currently pending in the subject application and are presently under consideration. Claims 1-6, 8, 19 and 21 have been amended as shown at pages 2-4 of the Reply.

Applicants' representative thanks Examiners Moazzami and Traore for the courtesies extended during the telephonic interviews conducted on January 23, 2007. Examiners were contacted to discuss the rejections under 35 U.S.C. §102(b) and 35 U.S.C. §103(a). During the interview a set of amendments were presented that the Examiners agreed overcame the rejections in view of cited art identified in the Office Action. These amendments have been incorporated into the claims as shown above. Examiner indicated that further search and consideration was required to determine if the claims would be allowed.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-3, 19, 21 and 22 Under 35 U.S.C. §102(b)

Claims 1-3, 19, 21 and 22 stand rejected under 35 U.S.C. §102(b) as being anticipated by Ayyagari, *et al.* (US 2002/0176366). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Ayyagari, *et al.* does not teach each and every element of applicants' invention as recited in the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2
> USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject claims relates to identification of the type of security encryption employed on a wireless network, for example, by detecting failures and timeouts during authentication. By recognizing failures or timeouts during particular portions of the authentication process, an iterative approach can narrow down the possible encryption types until identification of the encryption type being employed is achieved, without any user input or pre-stored information

regarding the network encryption type. In particular, independent claim 1 (and similarly independent claim 21) recites *a detection component that* ***automatically identifies an encryption type of an available wireless network****, wherein* ***identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network***.

Contrary to assertions in the Office Action, Ayyagari, *et al.* does not teach or suggest the aforementioned novel features as recited in the subject claims. The cited reference discloses a system for switching between available networks as a user moves to different locations without the user having to manually enter network connection information upon arrival at each location. This is accomplished by the system caching information when a user enters information the first time or providing a UI for the user to enter information for networks in advance as stored network preferences. The system employs beacon information received/downloaded from the network to identify available networks and uses the cached or stored information to connect to the known networks. If there are no known networks the system attempts to connect to ad hoc networks. When the system attempts to connect to a network and the connection fails, the system attempts to connect to a different network. The Office Action cited paragraphs [0011, 0051, and 0055] as teaching that the system employs failure during authentication to determine the encryption type of the network. Paragraph [0011] discloses that the system attempts to connect to a network, and if this connection fails, the system will attempt to connect to another network. Paragraph [0051] discloses that if the system is in Ad-Hoc mode and an SSID of an available network that has not previously failed becomes available, the system will attempt to connect to network associated with the SSID. Cited Paragraph [0055] discloses that the user selects authentication setting. With regards to Figure 6, elements 264 and 292 merely disclose that the system will perform a scan to identify which networks are available to the user and build a BSSID list of the available networks. Element 272 discloses that the user selects the authentication setting. These cited paragraphs and figures, as well as the entire reference, do not teach identifying the encryption type of the network based upon failure during the authentication sequence. Ayyagari, *et al.* is also silent regarding identifying the encryption type of the network based upon exceeding a time threshold during the authentication sequence. Therefore, Ayyagari, *et al.* fails to teach or suggest a detection component that automatically identifies an encryption

type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network.

Moreover, independent claim 19 recites *a data field comprising information identifying an encryption type of an available wireless network connection, wherein* ***identification of the encryption type of the available wireless network being based, at least in part, upon iterative probing of the available wireless network, wherein the iterative probing employs failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence to identify the encryption type***. As discussed above, Ayyagari, *et al.* does not attempt to identify the encryption type of a network based upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence to identify the encryption type. Moreover, the system does not employ any form of iterative probing of a network to determine the encryption type of the network. Ayyagari, *et al.* performs a scan to determine which networks are available and then may attempt to connect to each network until it is able to make a connection. As such, the cited reference fails to teach or suggest all features of the subject claim.

Furthermore, independent claim 22 recites *means for connecting a device to a plurality of wireless networks; and, means* ***for automatically identifying an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence***. As noted supra, Ayyagari, *et al.* is silent regarding identifying the encryption type of a wireless network based upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence to identify the encryption type.

In view of the foregoing, applicants' representative respectfully submits that Ayyagari, *et al.* fails to teach or suggest all limitations of independent claims 1, 19, 21, and 22 (and claims 2-3 that depend there from), and thus fails to anticipate the subject claims. Accordingly, withdrawal of this rejection is respectfully requested

II. Rejection of Claims 4-10, 12, 13 and 15-17 Under 35 U.S.C. §103(a)

Claims 4-10, 12, 13 and 15-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ayyagari, *et al.* (US 2002/0176366) in view of Krantz, *et al.* (US 2004/0111520). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Ayyagari, *et al.* and Krantz, *et al.* do not teach each and every element of applicants' invention as recited in the subject claims.

Claims 4-10 depend from independent claim 1. As noted *supra*, Ayyagari, *et al.* does not teach or suggest each and every element of the subject invention as recited in this independent claim, and Krantz, *et al.* fails to make up for the aforementioned deficiencies of Ayyagari, *et al.* Krantz, *et al.* discloses a system for allowing a user to connect to an ISP without requiring the user to have any previous knowledge about the requirements or have to call the ISP to connect to the ISP network. This is accomplished by redirecting the user to a URI that downloads a master document which contains information regarding the connection requirements for an ISP or by having this information pre-stored on the user's computer. In this manner, the master document is accessed to inform the user or configure the user for connection to the ISP. Krantz, *et al.* is silent regarding ***identification of the encryption type of an available wireless network based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network***.

In addition, claim 4 recites ***identification of the encryption type of the available wireless network by the detection component being based, at least in part, upon iterative probing of the available network***. Contrary to assertions in the Office Action, Krantz, *et al.* fails to teach this novel feature of the subject claim. The Office Action asserts that [0066] of Krantz, *et al.* discloses this feature. However, this paragraph merely discloses that the client will send probe requests in order to identify which networks are available and then employ responses from the available beacons to identify available SSIDs and their authentication and encryption types. This authentication and encryption information is included as part of the probe response from the beacon. Each available network will send a probe response. The cited reference does not teach iterative probing of ***an*** available network in order to determine its encryption type. One probe request per network is all that is required because the beacon will respond to the probe request providing the needed information.

Independent claim 12 recites *attempting to connect to a wireless network as a wireless provisioning services supporting network;* ***automatically identifying the encryption type of the wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; determining whether the attempt was successful; and, prompting for a wired equivalent privacy key, when the attempt was not successful***. As discussed above, Ayyagari, *et al*. does not attempt to automatically identify the encryption type of a network based upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence. Ayyagari, *et al*. discloses that the user selects the authentication setting. Furthermore, Ayyagari, *et al*. does not attempt to connect to a network using a first type of encryption (WSP) and when that is not successful employs a second type of encryption(WEP) to connect to the same network. Krantz, *et al*. also fails to disclose either of these features. Paragraph [0066] of the cited reference discloses that the system relies on the probe responses from beacons that inform the client of the encryption type of the wireless network associated with the beacon. The paragraph merely states that WEP is one of the encryption types as an example. Hence, the cited references fail to teach each and every feature of the subject claim.

Additionally, independent claim 15 recites ***determining whether a wireless network supports 802.1x, based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key when the wireless network does not support 802.1x; determining whether the wireless network supports wireless provisioning services when the wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; and, identifying the wireless network as an 802.1x network, when the wireless network does not supporting wireless provisioning services; and, identifying the wireless network as a wireless provisioning services supporting network, when the wireless network supports wireless provisioning services***. The subject claim discloses a sequential approach wherein failure of identification of one type of network is indicative of another network type. A specific narrowing sequence that checks for various network authentication types in sequential order until the authentication type of the network is identified. As previously discussed, both Ayyagari, *et al*. and Krantz, *et al*. fail to teach or suggest this

novel sequence for identifying the encryption type of a wireless network. Ayyagari, *et al.* discloses that the user selects the authentication setting. Cited pargraphs [0094 and 0098] of Krantz, *et al.* merely discloses elements of an XML file that define configuration settings for a wireless network. However, the system relies upon this XML document being download or stored on the client machine. The client machine will then employ the configuration settings to the connect to the network. The paragraphs do not disclose a sequence for determining the encryption type of the wireless network based upon failure or exceeding a threshold during authentication as discloses in the subject claim.

In view of at least the foregoing discussion, applicants' representative respectfully submits that Ayyagari, *et al.* and Krantz, *et al.*, alone or in combination, fail to teach or suggest all limitations of applicants' invention as recited in independent claims 1, 12 and 15 (and claims 4-10, 13, 16 and 17 that respectfully depend there from), and thus fails to make obvious the subject claimed invention. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP552US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/

Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731